EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Arthur Yuan on July 14, 2008.

Claims 1, 11 and 17 are amended as follows:

Claim 1 (currently amended): A method for authenticating a user certificate received from a user requesting access to a secure web service, said user certificate including user certificate data, said method comprising:

receiving a request from a user for access to the web service, said request including partial data supporting the user certificate data;

retrieving revoked certificate data from a plurality of certificate issuers, wherein the revoked certificate data identifies one or more revoked certificates, said each of the one or more identified revoked certificates including a next update time for retrieving an update to each of the revoked certificates and an address identifying a location for retrieving the update;

storing the revoked certificate data in a central location;

determining if the user certificate data has expired;

if the determining indicates that the received user certificate data has expired, denying the user accessing the secure web service;

if the determining indicates that the received user certificate data has not expired:

comparing the user certificate data included in the received request to the revoked certificate data stored in the central location;

if the comparing indicates that the user certificate data from the requested user certificate matches one of the revoked certificate data stored in the central location, denying the user access to the secure web service;

if the comparing indicates that the user certificate data from the requested user certificate does not match the revoked certificate data stored in the central location, determining if the update to one of the revoked certificates is available based on the next update time;

if the determining indicates that no update is available, authenticating the user to access the secured web service;

if the determining indicates that the update is available, retrieving the update from the address;

in response to the retrieved update, storing the update to one of the revoked certificates in the central location;

if the comparing indicates that the user certificate data matches the updated revoked certificate data in the central location, denying the user access to the secure web service;

if the comparing indicates that the user certificate data does not match one of the updated revoked certificate data in the central location:

authenticating the user;

providing the user access to the requested web service;

detecting an event including a new entry in the central location, a current time equals to the next update time of one of the revoked certificate data or the current time equals to the next update time of one of the updated revoked certificate data;

organizing the user certificate data in the revoked certificate data in a sequence according to the next update time for each of the plurality of certificate issuers; and

in response to the detected event and the next update time, retrieving another update of one of the revoked certificate in the central location according to the organized sequence.

Claim 11 (currently amended). A system for retrieving revoked certificate data in response to a client request, said client request requesting access to a secure web service and including user certificate data, comprising:

a central database;

a fetching server for retrieving revoked certificate data from a plurality of certificate authority servers for storage in said central database, wherein the revoked certificate data identifies one or more revoked certificates; and

an authentication server responsive to the client request for executing a certificate revocation provider component, said certificate revocation provider component loading the revoked certificate data in the central database into a memory associated with the authentication server, and wherein the certificate revocation provider component is responsive to the client request and loaded revoked certificate data to determine if the client request is authentic based on a match of the client request and the stored revoked certificate data,

wherein,

if the client request is expired, the authentication server denies the user;

if the client request is not expired and if a match of the client request and the stored revoked certificate data is not found; determining if the update to one of the revoked certificates is available based on the next update time;

if the determining indicates that no update is available, the authentication server authenticates the user to access the secured web service;

if the determining indicates that the update is available, the fetching server retrieves the update from the address;

in response to the retrieved update, the certification revocation provider component stores the update to one of the revoked certificates in the central database;

if the comparing indicates that the user certificate data matches the updated revoked certificate data in the central database, the authentication server denies the user access to the secure web service;

if the comparing indicates that the user certificate data does not match one of the updated revoked certificate data in the central database:

the authentication server authenticates the user;

the authentication server detects an event including a new entry in the central database, a current time equals to the next update time of one of the revoked certificate data or the current time equals to the next update time of one of the updated revoked certificate data;

wherein the fetching server organizes the retrieved revoked certificate data in a sequence according to the next update time for each of the one or more certificate authority servers; and

in response to the detected event and the next update time, the fetching server retrieves another update of one of the revoked certificate in the central database according to the organized sequence.

Claim 17 (currently amended): A system for managing certificate revocation status data, comprising:

a fetching server for identifying a list of addresses corresponding to a plurality of certificate issuers, said fetching server retrieving revoked certificate status data from a content server corresponding to the list of addresses; and

a central database responsive to the retrieved revoked certificate status data for storing a list of revoked certificates,

wherein if the comparing indicates that the user certificate data from the requested user certificate does not match the revoked certificate data stored in the central location, determining if the update to one of the revoked certificates is available based on the next update time;

if the determining indicates that no update is available, authenticating the user to access the secured web service;

if the determining indicates that the update is available, retrieving the update from the address;

in response to the retrieved update, storing the update to one of the revoked certificates in the central location;

if the comparing indicates that the user certificate data matches the updated revoked certificate data in the central location, denying the user access to the secure web service;

if the comparing indicates that the user certificate data does not match one of the updated revoked certificate data in the central location:

authenticating the user;

providing the user access to the requested web service;

detecting an event including a new entry in the central location, a current time equals to the next update time of one of the revoked certificate data or the current time equals to the next update time of one of the updated revoked certificate data; and

wherein the fetching server organizes the retrieved revoked certificate data in a sequence according to the next update time for each of the one or more certificate issuers;

in response to the detected event, retrieving another update of one of the revoked certificate in the central location; and

wherein the fetching server identifying a address from a user certificate data included in a client request for the stored the list of revoked certificates if it is determined that there is no match between the user certificate data and retrieved certificate status data, said address identifying the location of revoked certificate data for a plurality of revoked certificates being maintained by at least one of the plurality of certificate issuers, and wherein the central database stores the address in the central location for subsequent retrieval according to the next update time in the organized sequence.

Claim 18 (currently amended): A computer storage medium comprising computer-executable instructions for authenticating a user requesting access to a web service, comprising

retrieving instructions for retrieving revoked certificate data from a plurality of certificate issuers, wherein the revoked certificate data identifies one or more revoked certificates;

storing instructions for storing the revoked certificate data for each of the identified one or more revoked certificates in a central location;

receiving instructions for receiving a request from a user for access to the web service, said request including a user certificate including user certificate data;

comparing instructions for comparing the user certificate data to the revoked certificate data stored in the central location;

denying instructions for selectively authenticating the user if the comparing indicates that the user certificate data matches the revoked certificate data in the central location;

if the comparing indicates that the user certificate data from the requested user certificate does not match the revoked certificate data stored in the central location:

determining instructions for determining if the update to one of the revoked certificates is available based on the next update time;

if the determining indicates that no update is available, authentication instructions for authenticating the user to access the secured web service;

if the determining indicates that the update is available, retrieving instructions for retrieving the update from the address;

in response to the retrieved update, storing instructions for storing the update to one of the revoked certificates in the central location;

wherein the authentication instructions authenticate the user;

wherein the providing instructions provide the user access to the requested web service;

identifying instructions for identifying an address from the user certificate data included with the request, said address identifying the location of revoked certificate data for a plurality of revoked certificates being maintained by at least one of the plurality of certificate issuers;

organizing instructions for organizing the retrieved revoked certificate data in a sequence according to the next update time for each of the one or more certificate authority servers; and

wherein the storing instructions store the address in the central location for subsequent retrieval according to the next update time in the organized sequence.

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance: the limitation of organizing the retrieved revoked certificate data in a sequence according to the next update time of the certificate authority distinguishes the claimed invention over the prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CORDELIA KANE whose telephone number is (571)272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/C. K./
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132